

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

The residence located at 66 Orchard View Court, Howard,
Ohio 43028 including any curtilage, a 2013 Black Ford
Fusion, license plate # HZT3598 and any/all persons,
computers and/or digital media located therein/thereon

Case No. 2:20-mj-340

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC Sec. 2251

Offense Description
Production/attempted production of child pornography

18 USC Secs 2252 and 2252A Receipt/possession/distribution of child pornography/visual depictions of minors engaged in sexually explicit conduct in interstate commerce

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Josh Saltar, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/12/2020City and state: Columbus, Ohio

Judge's signature

Chelsey M. Vascara, U.S. Magistrate Judge

Printed name and title



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

IN THE MATTER OF THE SEARCH OF: The residence located at 66 Orchard View Court, Howard, Ohio 43028 including any curtilage, a 2013 Black Ford Fusion, license plate # HZT3598 and any/all persons, computers and/or digital media located therein/thereon	Case. No. ----- Magistrate Judge:
--	--

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Josh Saltar ("your affiant"), a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a SA with the FBI and have been since October 2014. I am currently assigned to the Cincinnati Field Office, Violent Crimes Against Children Squad investigating matters involving the online exploitation of children and child pornography, and I am trained and authorized to investigate the offenses alleged herein.

2. During my career as a SA, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses involving children. I have also received formal training from industry leading forensic examiners and cyber incident responders. As part of my duties as a SA, I investigate criminal child exploitation and child pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A.

3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts believed to be necessary to establish probable cause for a search warrant for the premises of 66 Orchard View Court, Howard, Ohio 43028 (hereinafter the “**PREMISES**”), and a vehicle described as a Black 2013 Ford Fusion – Tag # HZT3598 (hereinafter the “**VEHICLE**”). I have not withheld any evidence or information which would negate probable cause.

5. The **PREMISES** and **VEHICLE** to be searched is/are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A – the production/attempted production, distribution, transmission, receipt, and/or possession of child pornography.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit

conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

8. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

9. As it used in 18 U.S.C. §§ 2251 and 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

10. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

11. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

12. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”

13. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.

14. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”

15. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

IV. BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES, AND THE INTERNET

16. I have both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

17. Computers and computer technology have revolutionized the way in which child pornography is produced and distributed. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

18. The development of computers and mobile computing devices (smart phones, tablets, and electronic storage media, hereinafter referred to as “mobile devices” or “digital devices”) has

added to the methods used by child pornography collectors to interact with each other and/or to sexually exploit children. Computers and mobile devices serve four functions in connection with child pornography: production, communication, distribution, and storage.

19. Pornographers used to produce still and moving images with cameras/video cameras and/or transfer images using a scanner. The camera or scanner was attached directly to the computer and the files could be stored, manipulated, transferred or printed using the computer. The captured videos or images could be edited in very similar ways to a photograph (lightened, darkened, cropped, or manipulated). Although these methods are still used, now mobile devices have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as did the production methods that had been used in the past.

20. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market child pornography. The development of the computer, mobile computing devices, and the Internet, has also changed that.

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers or cellular network; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting

information, account application information, Internet Protocol (“IP”) addresses² and other information both in computer data format and in written record format.

22. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user’s true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

23. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person “deletes” a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

24. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file

² The IP address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. When mobile devices connect to the Internet they are assigned an IP address either by the residential/commercial WiFi ISP or the cellular ISP. The IP address assignments are controlled by the respective provider.

from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

25. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

26. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including GIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

27. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

28. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage

capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Tablets and laptop computers are also easily transferred from one location to another, and may be transferred in a carrying case on the person of an individual or in a vehicle. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

29. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto

opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

- Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

32. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, and 2252A, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

33. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment B;
- searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;
- surveying various files, directories and the individual files they contain;
- opening files in order to determine their contents;
- scanning storage areas;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

VII. INVESTIGATION AND PROBABLE CAUSE

34. On February 5, 2020, a case worker at Nationwide Children's Hospital contacted Mount Vernon Police Department (MVPD) regarding a possible sexual assault on a 3-year-old victim (VICTIM). VICTIM's mother informed the case worker that on February 4, 2020, VICTIM told her that when Tyler Smith (SMITH) was changing her diaper, he put "his butt to her butt." As she was making this statement, VICTIM pointed to her vagina. VICTIM's mother advised that VICTIM was currently being toilet trained and refers to her private areas as "butt". VICTIM went on to tell her mother that her "butt" hurt after the encounter.

35. On February 6, 2020, MVPD went to VICTIM's residence and spoke with VICTIM'S mother. The mother showed MVPD officers the text messages between SMITH and the mother that had been exchanged on February 5. In the messages, SMITH asked the mother not to make a report or say something she would regret to Children Protective Services. He further stated that if she made a report that it could make him go to prison, or that he would take his own life. He went on to state that the incident did not happen recently and that it was a mistake, as well as referring to himself as a repeat offender.

36. VICTIM's mother turned over two tablets and a laptop computer to MVPD that she found within her residence. She stated that she could not find the laptop computer that belonged to

SMITH that had previously been in the residence. She stated that SMITH had been at her residence at some point while she was at Nationwide Children's Hospital on February 5, after SMITH's mother had requested that SMITH be permitted to obtain some of SMITH's belongings that were at the house. Additionally, VICTIM's mother stated that the trash was taken out when she returned from the hospital and suggested that SMITH was responsible for that. Neither Smith nor the vehicle that he drove were at VICTIM's mother's house when MVPD were there, and VICTIM's mother had informed MVPD that SMITH was to be staying at his parents' residence but had checked himself into the local hospital after she called the children's services agency.

37. On February 6, 2020, after speaking with VICTIM's mother, MVPD went to Knox Community Hospital to speak with SMITH. Also present in SMITH's room were his parents, Ben (BEN) and Sally (SALLY) Smith. BEN advised that they had retained an attorney, and had advised that SMITH not speak to MVPD at that time. MVPD requested that SMITH turn over his cell phone for the investigation, which he agreed to do.

38. On March 26, 2020, four state search warrants were signed for the devices seized from VICTIM's mother and SMITH by Knox County Sheriff's Office Detective Daniel Bobo. Copies of the warrants and the four devices were then transferred to your affiant to provide assistance with forensic imaging and review. Additionally, Detective Bobo provided a prior case report that showed on November 11, 2012, SMITH was convicted of the following charges: Sections 2907.321(A)(1) and 2923.02(A) of the Revised Code of Ohio - Attempted Pandering Obscenity Involving a Minor, and Sections 2907.322(A)(1) and 2923.02(A) of the Revised Code of Ohio - Attempted Pandering Sexually Oriented Matter Involving a Minor.

39. Your affiant conducted a forensic examination of SMITH's cellular phone utilizing various forensic tools, as well as manually reviewing the phone. The initial forensic examination revealed the following texts between SMITH and VICTIM's mother that were exchanged on February 4 and 5, 2020:

- SMITH: Stay or leave?
- SMITH: What do you want me to do
- VICTIM's mother: I will comedown in a minute
- SMITH: Please be careful what you say and who you sat it to. Your words have the power to destroy everything right now, including taking my life. Please don't say anything you will regret. We need to talk about this between us first
 - VICTIM's mother: Well maybe you should of thought of that in the beginning. You had a chance to talk last night and you didn't. I have lost all hope and all trust in you. This is to big for me to not say anything. I have to protect

[VICTIM] and myself, I will be calling social services and we can talk with them.

- SMITH: You do know that could end with me in prison for the rest of my life, right? This isn't just going to blow over. There will be tons of questions, and investigation, and they could lock me up immediately. It will be very ugly for all of us. This will affect more than just me and you. Both our families will be devastated. I don't think you understand how serious this can get

- SMITH: How is calling them going to protect anyone? They will make our lives hell, worse than you believe it is already.

- SMITH: Please don't call them

- SMITH: I am pleading with you, spare my life

- VICTIM's mother: I do understand and I have Been thinking about everything all night. maybe you should have thought of that first, because apparently that doesn't stop you. It will prevent this from happening again and get us the help we need. Tyler, this is to big for me to sit back and do nothing. I cannot let it happen again.

- SMITH: Leave me if you have to, but please don't end my life

- SMITH: How is me being in jail/prison going to help us

- VICTIM's mother: I am liable now and if i don't say anything I could go to jail too

- SMITH: I know. Just please reconsider your actions. This could end VERY badly for both of us. Especially me

- VICTIM's mother: What exactly do you propose that I do then?

- SMITH: Literally anything else but that. Idk what. This wasn't something that happened recently, either. At least consider that. Consider how I've been fighting to be a better person. Think of the changes in my life you've seen in me. This was a mistake I made a while ago, and I have been fighting to change. And I have. I know you may not have any reason to believe that anymore, but I have changed. I really am fighting this. I have mood swings, but that's really just my flesh fighting back. This is something that has been a part of me my whole life, it's going to take time and effort to get rid of it. Please don't give up on me and throw away everything we have. Our life together. Our plans for a better future for all of us. Realize what the future may very well be like if CPS gets involved. Separation, divorce, jail, prison, 2 daughters with no father... I really don't believe you want that. Please just give yourself time to think about this and not react out of fear. I know you believe it will help, but I seriously doubt it will go like you think. It won't just be counseling and leadership. They will get the law involved. And they don't play games and give second chances. Especially for someone who is a repeat offender. This CAN be handled another way.

- SMITH: Sexual addiction counseling

- VICTIM's mother: You've been talking about counseling for 5 years now and still have yet to start

- SMITH: I know, but I've never been to a specialist
- VICTIM's mother: I'm really sorry, but I did call. I cannot be held liable for this and it is very serious. They have started an investigation and you are not aloud in the house until it's over. The social worker will be calling you. I am thinking you can either go to your parents or a hotel
- SMITH: You have seriously put my life in danger of ending today. This could have been handled differently. I really wished you would have not done that
- VICTIM's mother: It is not ok what you did and I am not going to just let it go
- SMITH: I never said "just let it go"
- VICTIM's mother: You are the one that made the choice and brought this on us so don't play the victim card
- SMITH: This could have been handled differently, it didn't have to go this far
- VICTIM's mother: I need to tell them where your gonna stay at least for tonight
- SMITH: Idk yet. I'm meeting up with my dad now to talk. I'll let you know. Probably at his house, unless he doesn't want me to
- VICTIM's mother: Ok
- VICTIM's mother: I need to know where your staying within the next hour
- SMITH: My dads
- VICTIM's mother: Are you at your parents?
- VICTIM's mother: Thank you for putting the trash out

40. Continued review of SMITH's cell phone identified the following texts between SMITH and BEN on February 5, 2020:

- SMITH: Are you at work
- BEN: Yep
- BEN: Wsup
- BEN: [Smile emoji]
- BEN: Yo
- SMITH: I messed up bad and I'm in trouble. [VICTIM's mother] called CPS. I'm not allowed to go home. I fear for my life, and my future. I have nowhere to go. My life could very well be over today. I'm so sorry I have to tell you this. I don't know who else to turn to. I don't want to drag you into my mess, but you would have found out eventually.
- BEN: What. Where are you
- SMITH: Work, for now.
- BEN: Lunch break
- BEN: ?
- SMITH: Sure. I won't be able to eat
- BEN: When,

- SMITH: Whenever. Now, I suppose. Not like it's going to matter if this goes south.
- BEN: I'll be there in a minute
- BEN: I'm here

41. Continued analysis of SMITH's cell phone revealed what appeared to be two applications designed to wipe data from a cell phone: ishredder³ and easymemorycleaner⁴.

42. Your affiant identified a document titled "iShredder_Report.pdf" found on the phone. The report appeared to be created from the iShredder application, and indicated that on February 3, 2020 at 2:47 PM, the iShredder application ran, and the result section indicated that it was successfully run on "Files Vaulty". Additionally, your affiant identified the password protected application Vaulty⁵ on the device. Your affiant was able to access the application, however there were no files or folders in the application, which indicated that the iShredder application was likely run on the files in that application.

43. Your affiant identified two files, "last_cleaning_date" and "auto_clean", as belonging to the application easymemorycleaner. Your affiant decoded the data in the last_cleaning_date file and found the value February 3, 2020 7:41:51 -0500, which indicated that the application was last run on that date. Your affiant decoded the data in the auto_clean file and found the value "false", which indicated that the application had to be manually run by the user and not automatically run by the phone.

44. The forensic examination of SMITH's phone was also able to recover remnants of three apparently child pornography images that had been deleted from the phone. The images were depicted a female, approximately 13 years old, in the bathroom. The girl had her pants and underwear around her knees, and her vagina was fully exposed. The picture appeared to be taken from a wide-angle fisheye lens located in the corner of the bathtub. Additionally, your affiant identified a PDF file titled "aacbddf7-002d-4094-b894-0151d7b6e3b3.pdf". The file was a user guide for a Camscura Tilt Hidden Camera, created by BrickHouse Security. According to

3 Open source research of the iShredder app on the Google Play store showed it was created by ProtectStar, Inc., and claimed "with military-grade security, iShredder(TM) data shredder (eraser) app which securely deletes data leaving them irrecoverable and protects falling into malicious hands".

4 Open source research of the easymemorycleaner app on the Google Play store showed it was created by J Kosa, and claimed "Powerful cleanup of memory. Just one tap to start. Special knowledge and settings are NOT needed!".

5 Open source research of the Vaulty app on vaultyapp.com showed it was created by Squid Tooth LLC, and claimed "Do you have pictures or videos on your phone that you don't want others to see? Hide pictures & private videos with Vaulty to keep them protected from prying eyes. Keeping pictures & videos safe, secure and hidden has never been easier!".

brickhouse.com, the Camscura Tilt Hidden Camera was a “covert cam with an adjustable lens [that] hides in plain sight in your home or office.” On May 6, 2020, Detective Bobo showed the images to VICTIM’s mother, who confirmed that the bathroom in the picture was the bathroom in SMITH’s house, and that the girl in the photo was SMITH’s minor female relative.

45. Your affiant then reviewed the phone manually and identified an app titled Keep Notes⁶, and identified two notes that appeared to be written by SMITH. The first note was titled “Why I need counseling”, and the following is an excerpt from the note:

"I have tried in the past multiple times to stop all those things with very short term success. I have been jailed for 3 months and am currently a tier 2 registered sex offender for downloading and possessing thousands of nude/sexual photos and videos of minors, and conducting voyeurism in public restrooms. It still did not stop me. I have continued to download photos and videos and still participated in voyeurism within my circle of family/friends, taking photos and videos of minors without their knowledge."

46. The second note was titled "Things I want most in life", and the following is an excerpt from the note:

"I want my new phone back already. In complete working condition, with no microphone problems. But yet, it's been over a week, and I'm still waiting. All the while worried as FUCK that SOMEHOW they got into my phone's memory and saw what shit I was downloading. Even though I secure erased it TWICE and did a factory reset TWICE."

47. In the review of the microSD card that was in SMITH’s cell phone, the data recovery tool Zero Assumption Recovery (ZAR)⁷ was used to recover files currently on the device as well as any files that might have been deleted. ZAR was able to recover nine deleted child pornography videos. One of the videos, approximately 6 minutes long, depicted a white female, approximately ten to eleven years old wearing a white shirt and nude from the waist down with her legs spread and exposing her vagina. The video appeared to be taken by the girl. The girl zoomed in on her vagina and began masturbating with a marker and inserting the marker into her vagina. The girl

⁶ Open source research on the Google Play store showed it was created by Google LLC, and claimed "Add notes, lists, and photos to Google Keep. Pressed for time? Record a voice memo and Keep will transcribe it so you can find it later".

⁷ According to <https://www.z-a-recovery.com/>, ZAR Data Recovery is suitable for home users and small businesses who need a powerful data recovery solution for Windows FAT, NTFS, Linux ext/2/3/4, and XFS file systems. The default settings are reliable and thorough, but more technical users can benefit from a wealth of optional configurations.

then got up and walked to the bathroom to sit on the toilet. The camera again zoomed in on her vagina while she urinated. Later in the video, the girl lifts up her shirt multiple times, exposing her breasts. A second video, approximately 45 seconds long, depicted a white female, approximately ten to eleven years old wearing a bathing suit top and nude from the waist down with her vagina exposed. The video appeared to be taken by the girl. The girl began masturbating. The girl then turned around and bent over, exposing her vagina and anus and continued masturbating. The girl turned back around and pulled her bathing suit top down, exposing her breasts. All the files had been deleted from the microSD card.

48. Continued review of the microSD card identified 115 deleted .vdata files that had been previously located in the subdirectory Documents\Vaulty\data. Open source research identified .vdata files as files created by the Android application Vaulty. Your affiant was able to decode the files, and found approximately 34 images that depicted what appeared to be a white female teenager in various stages of undress taking a shower, approximately 39 images that depicted what appeared to be a white female teenager in various stages of undress going to the bathroom, and approximately 7 images that appeared to be child pornography. One image depicted a white female teenager posing on a rug nude, with breast and vagina exposed. A second image depicted a white female teenager standing nude except for black underwear, with her breasts fully exposed. All the files had been deleted from the microSD card.

49. Open source research conducted through LexisNexis Accurint on May 4, 2020 identified **PREMISES** as the residence of SMITH, BEN, and SALLY. Additional open source research identified **VEHICLE** as registered to SMITH. Open source research conducted through OHLEG on May 11, 2020 confirmed the **PREMISES** and **VEHICLE** information above.

50. On May 4, 2020 at approximately 1:50pm, your affiant went to SMITH's place of business, Alene Candles, 8860 Smith's Mill Road, New Albany, Ohio 43031. In the parking lot, your affiant identified **VEHICLE**, which indicated that SMITH still owned and operated that **VEHICLE** and was using it as his means of transportation to and from work.

51. Based on the information provided, your affiant has reason to believe that SMITH likely removed devices that were present at VICTIM's residence after VICTIM's mother contacted CPS and prior to going to stay at **PREMISES**, and that the devices are likely located at **PREMISES** or in **VEHICLE**. Additionally, your affiant has reason to believe that the devices removed are likely to contain communications and images which may constitute contraband and evidence of criminal violations of 18 U.S.C. §§ 2251, 2252(a), and 2252A. Finally, your affiant has reason to

believe that because of SMITH's attempts to destroy contraband and evidence of the previously mentioned violations from his cellular phone, any of SMITH's devices that may be found at **PREMISES** or in **VEHICLE** may also contain evidence of attempts at destruction of evidence.

VIII. CHILD SEXUAL EXPLOITATION OFFENDER CHARACTERISTICS

52. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who produce, distribute, and receive child pornography:


- Those who exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- Those who exchange or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- Those who exchange or collect child pornography often times possess and maintain any their child pornographic material (pictures, videos, magazines, correspondence, mailing lists, books, child erotica, etc.) in the privacy and security of their homes or some other secure location. Child pornography distributors/collectors typically retain pictures, videos, magazines, correspondence, books, mailing lists, and child erotica for many years. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- Likewise, those who exchange or collect child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

- Those who exchange or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- Those who exchange or collect child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.
- When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

53. Based upon the conduct of individuals involved who communicate about and engage in online sexual abuse of children and exchange or collect child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of production, distribution and possession of child pornography is currently located on the **PREMISES** or in **VEHICLE**.

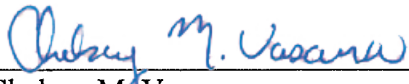
IX. CONCLUSION

54. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2252, 2252A, and 2251 have been committed, and evidence of those violations is located on the **PREMISES** or in **VEHICLE** described in Attachment A, and on any computers or computer related media found within. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment B.



Josh Saltar
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 12th day of May, 2020.



Chelsey M. Vascara
United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A

PROPERTY TO BE SEARCHED

The place to be searched is the residence and vehicle described below, including all its appurtenances, parking areas, outdoor working areas, detached buildings, individuals at the residence who may be in possession of a mobile computing device, and any computing related devices or digital media located therein or thereon.

The address 66 Orchard View Court, Howard, Ohio 43028, pictured below, is described on the Knox County Auditor's website as a split-level home on .77 acres of land:



The vehicle 2013 Black Ford Fusion with tag # HZT3598 is pictured below:



ATTACHMENT B
PROPERTY TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252, and 2252A:

1. Computer(s) and any digital media, computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in children or child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the production, possession, receipt, or distribution of child pornography, or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography, visual depictions of minors engaged in sexually explicit conduct, or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions of minors engaged in sexually explicit conduct.

6. Any and all notes, documents, records, or correspondence, in any format or medium

(including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography or any visual depictions of minors engaged in sexually explicit conduct.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the production, receipt, transmission, or possession of child pornography or visual depictions of minors engaged in sexually explicit conduct, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that shows connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

10. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.

11. Any and all cameras, film, videotapes or other photographic equipment, including cellular phones.

12. Any and all visual depictions of minors, for comparison to any visual depictions of minors engaged in sexually explicit conduct, child pornography, or child erotica found during the execution of this search warrant or sent during the course of this investigation.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters,

papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, or acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, of any child pornography or any visual depictions of minors engaged in sexually explicit conduct.

14. Any and all diaries, notebooks, notes, and any other records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.